

FIG. 1

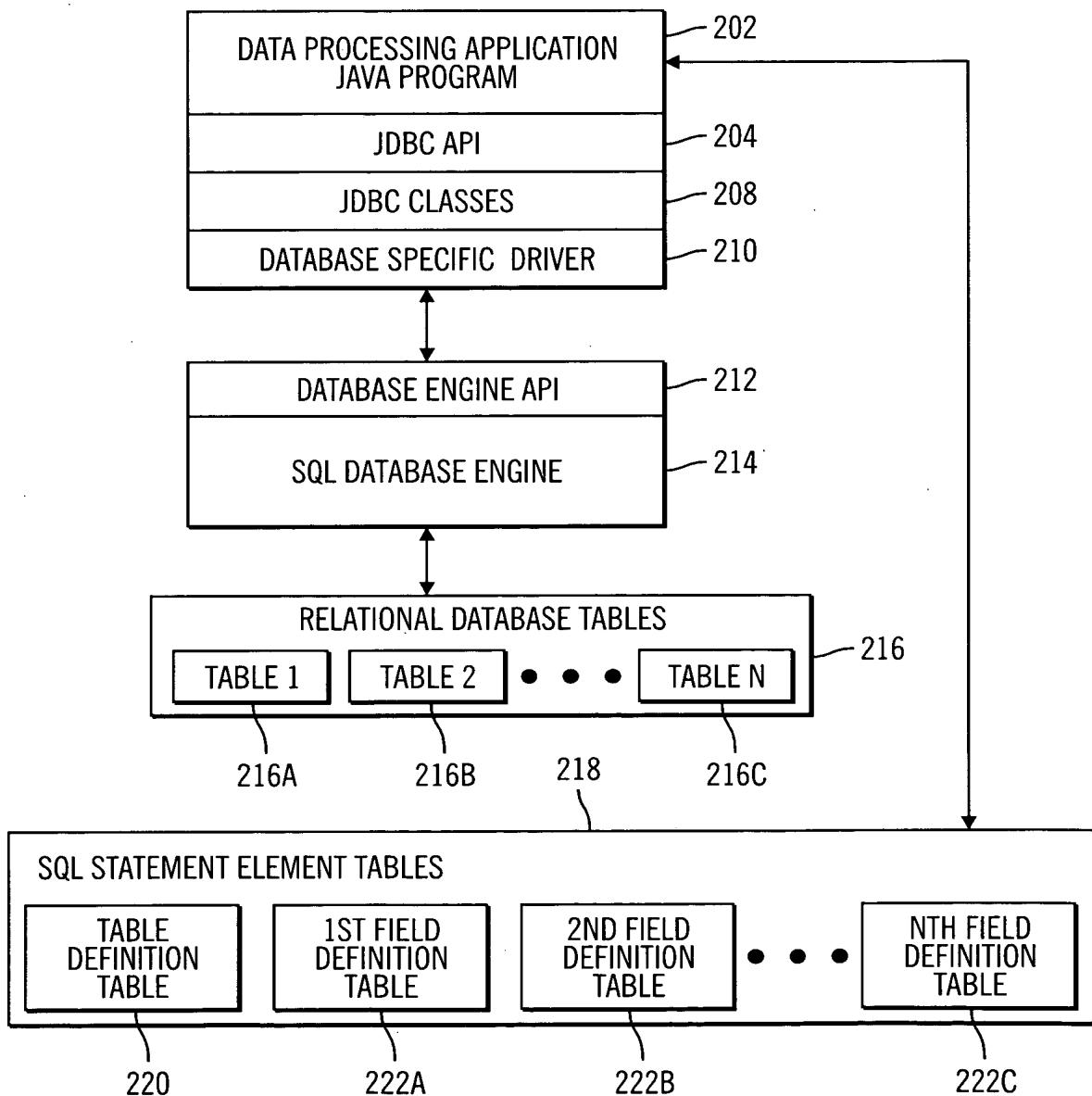
200

FIG. 2

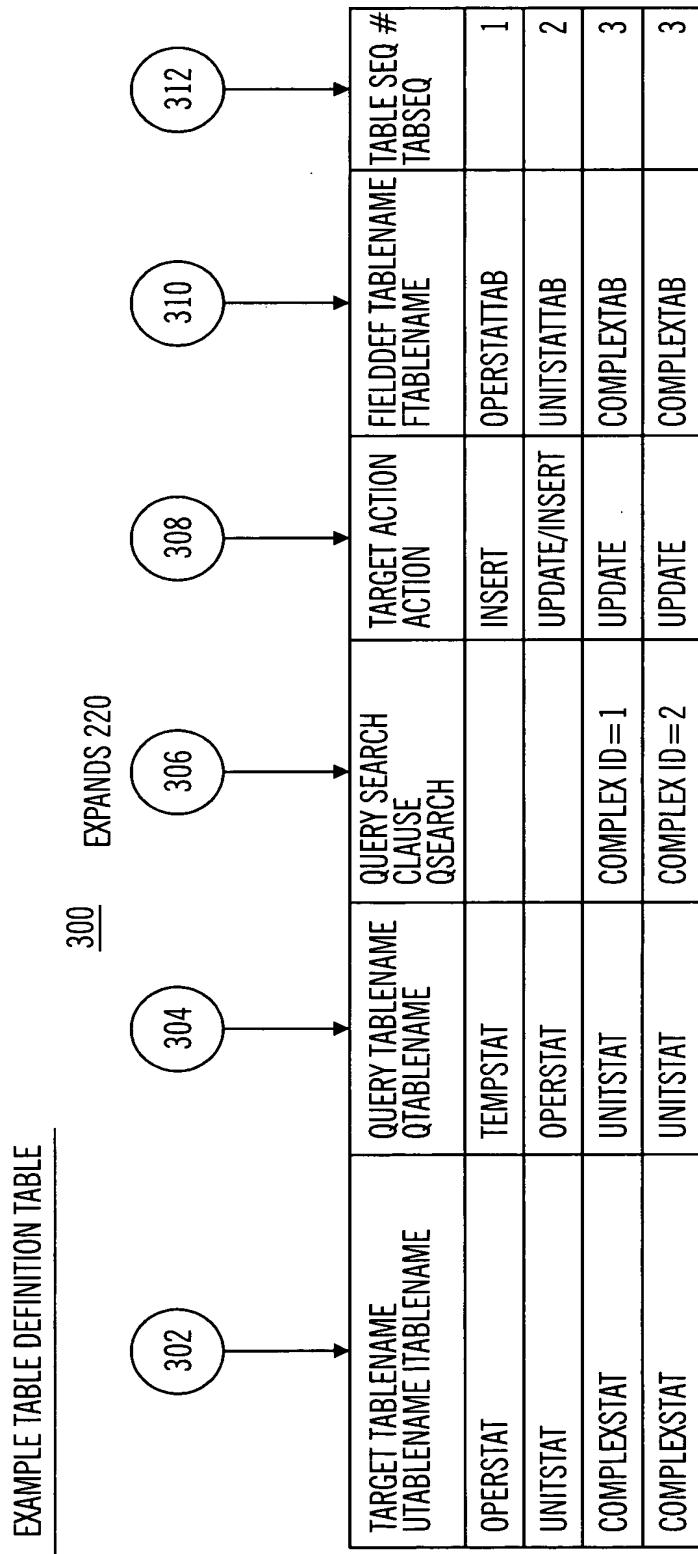


FIG. 3

EXAMPLE FIELD DEFINITION TABLES

FIELD DEFINITION TABLE: OPERSTAT

TARGET FIELD NAME TFIELD	QUERY SELECT CLAUSE SCLAUSE	QUERY GROUPBY CLAUSE GCLAUSE	UPDATE SET CLAUSE UCLAUSE	UPDATE WHERE CLAUSE WCLAUSE	INSERT FIELD CLAUSE ICLAUSE	FIELD JAVA TYPE JTYPE	SELECT FIELD SEQ # SELD SEQ	TARGET FIELD SEQ# TFLDSEQ
COMPLEX	COMPLEX				COMPLEX	STRING	1	1
UNIT	UNIT				UNIT	STRING	2	2
OPER	OPER				OPER	STRING	3	3
SHIFTS	SHIFTS				SHIFT	INT	4	4
CALLS	OPER				CALLS	INT	5	5
WRKTIME	WRKTIME				WRK TIME	INT	6	6

400 EXPANDS 222A

418 FIG. 4A

416

414

408

406

404

402

4/19

420 EXPANDS 222B

TARGET FIELD NAME TFIELD	QUERY SELECT CLAUSE SCLAUSE	GROUPBY CLAUSE GCLAUSE	UPDATE SET CLAUSE UCLAUSE	UPDATE WHERE CLAUSE WCLAUSE	INSERT FIELD CLAUSE ICLAUSE	FIELD JAVA TYPE JTYPE	SELECT FIELD SEQ # SFLD SEQ	TARGET FIELD SEQ # TFLDSEQ
COMPLEX	COMPLEX			COMPLEX = ?	COMPLEX	STRING	1	1
UNIT	UNIT	UNIT		UNIT = ?	UNIT	STRING	2	2
CALLS	SUM(CALLS)		CALLS = ?		CALLS	INT	3	3
WRK TIME	SUM(WRKTIME)		WRKTIME = ?		WRKTIME	INT	4	4
CUMCALLS			CUMCALLS = CUMCALLS + ?		CUMCALLS	INT	3	5
CUMWRKTIME			CUMWRKTIME = CUMWRKTIME + ?		CUMWRKTIME	INT	4	6

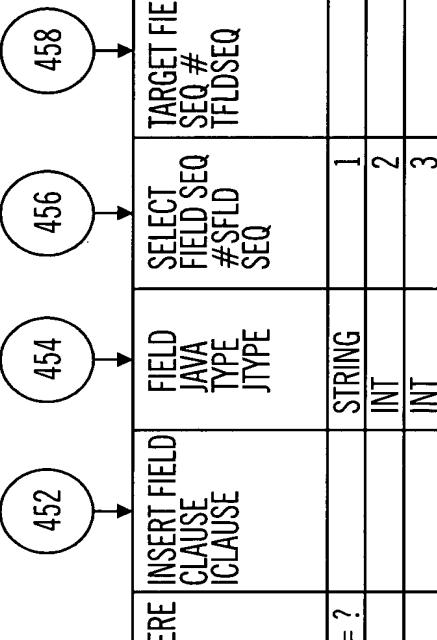


5/19

FIELD DEFINITION TABLE: COMPLEXSTATTAB

440 EXPANDS 222C

TARGET FIELD NAME TFIELD	QUERY SELECT CLAUSE SCLAUSE	GROUPBY CLAUSE GCLAUSE	UPDATE SET CLAUSE UCLAUSE	UPDATE WHERE CLAUSE WCLAUSE	INSERT FIELD CLAUSE ICLAUSE	FIELD JAVA TYPE JTYPE	SELECT FIELD SEQ # SFLD SEQ	TARGET FIELD SEQ # TFLDSEQ
COMPLEX	COMPLEX			COMPLEX = ?		STRING	1	1
CALLS	SUM(CALLS)		CALLS = CALLS + ?			INT	2	2
HRSWORK	SUM(WRKTIME)		HRSWORK = HRSWORK + ?			INT	3	3



+

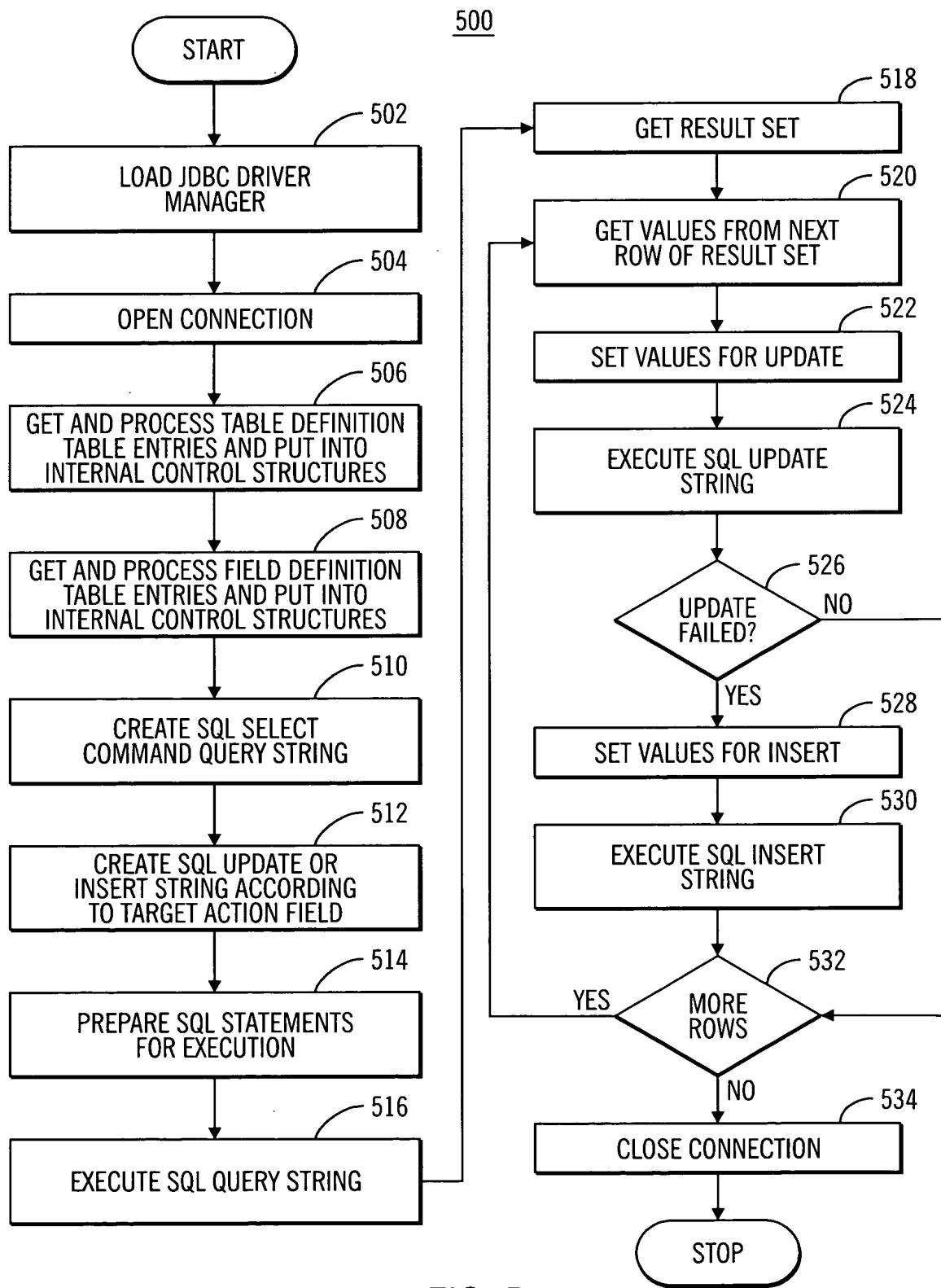


FIG. 5

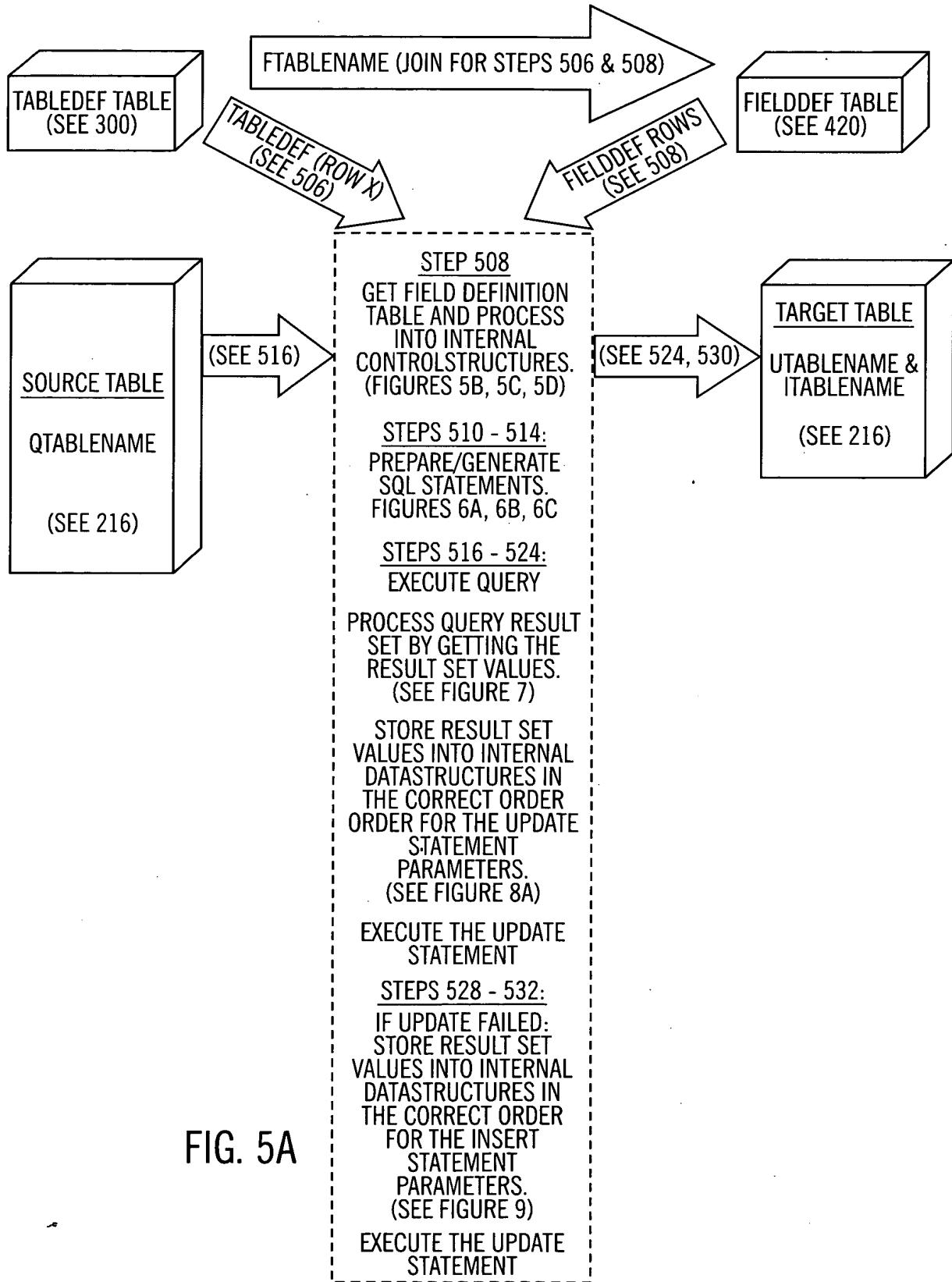


FIG. 5A

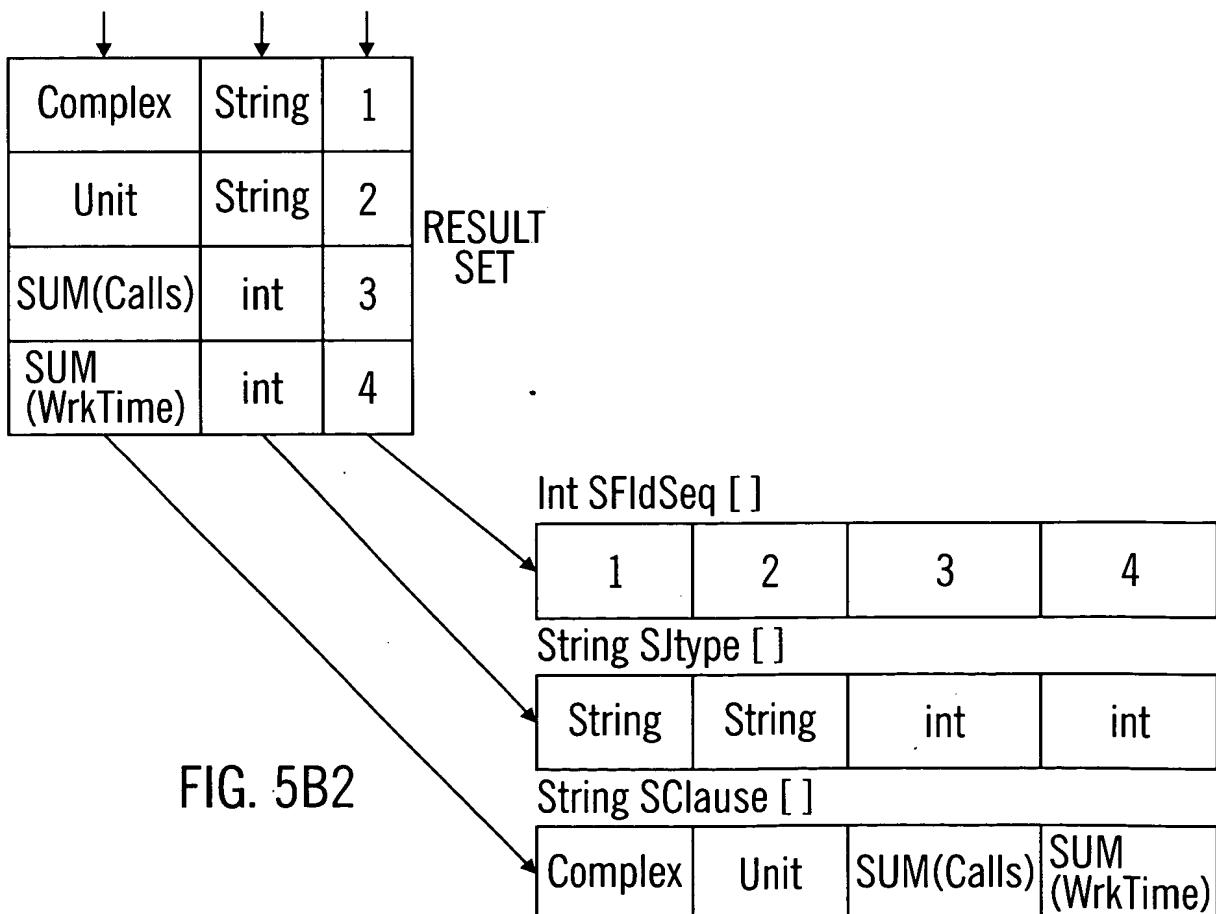
8/19

550

Select SCLAUSE, JTYPE, SFIDSEQ FROM UnitStatTab WHERE SCLAUSE is
NOT NULL ORDER BY SFIDSEQ

```
i=1
While not end of resultset
{
// Get values from next row of resultset
SClause[i] = GetString [1]           // get SCLAUSE
SJType[i] = GetString [2]            // get JTYPE
SFIdSeq[i] = GetInt [3]             // get SFIdSeq
i++
}
Ssize = i--:
```

FIG. 5B1



+

+

9/19

556

Select GCLAUSE, SFLDSEQ FROM UnitStatTab WHERE GCLAUSE is
NOT NULL ORDER BY SFLDSEQ

```
i=1
While not end of resultset
{
// Get values from next row of resultset
GClause[i] = GetString [i]           // get GCLAUSE — 557
i++
}
Gsize = i--:
```

FIG. 5B3

SELECT GCLAUSE, SFLDSEQ FROM UnitStatTab WHERE GCLAUSE is
NOT NULL ORDER BY SFLDSEQ

The diagram illustrates the flow of data. It starts with a SELECT query at the top, which points down to a 'RESULT SET' box. This box contains a table with two rows: 'Complex' and 'Unit'. The 'Complex' row has a value '1' in its second column, and the 'Unit' row has a value '2' in its second column. A diagonal arrow originates from the bottom right corner of the 'RESULT SET' box and points towards a 'String GClause []' box at the bottom right.

Complex	1
Unit	2

FIG. 5B4

String GClause []

Complex	Unit
---------	------

+

10/19

565

SELECT UCLAUSE, JTYPE, SFLDSEQ, TFLDSEQ FROM UnitStatTab WHERE
UCLAUSE is NOT NULL ORDER BY TFLDSEQ

i=1

While not end of resultset

{

// Get values from next row of resultset

UClause[i] = GetString [1] // get UCLAUSE

UJType[i] = GetString [2] // get JTYPE ————— 566

USFIdSeq[i] = GetInt [3] // get SFldSeq

UFldseq[i] = i // reset sequence

i++

}

Usize = i--:

FIG. 5C1

SELECT UCLAUSE, JTYPE, SFLDSEQ, TFLDSEQ FROM UnitStatTab WHERE UCLAUSE
is NOT NULL ORDER BY TFLDSEQ

Calls=?	int	3	3
WrkTime=?	int	4	4
CumCalls= CumCalls+?	int	3	5
CumWrkTime= CumWrkTime+?	int	4	6

RESULT
SET

Int UFldSeq []

1	2	3	4
---	---	---	---

Int USFIdSeq []

3	4	3	4
---	---	---	---

String UJtype []

int	int	int	int
-----	-----	-----	-----

String UClause []

Calls=?	WrkTime=?	CumCalls= CumCalls+?	CumWrkTime= CumWrkTime+?
---------	-----------	-------------------------	-----------------------------

FIG. 5C2

11/19

574

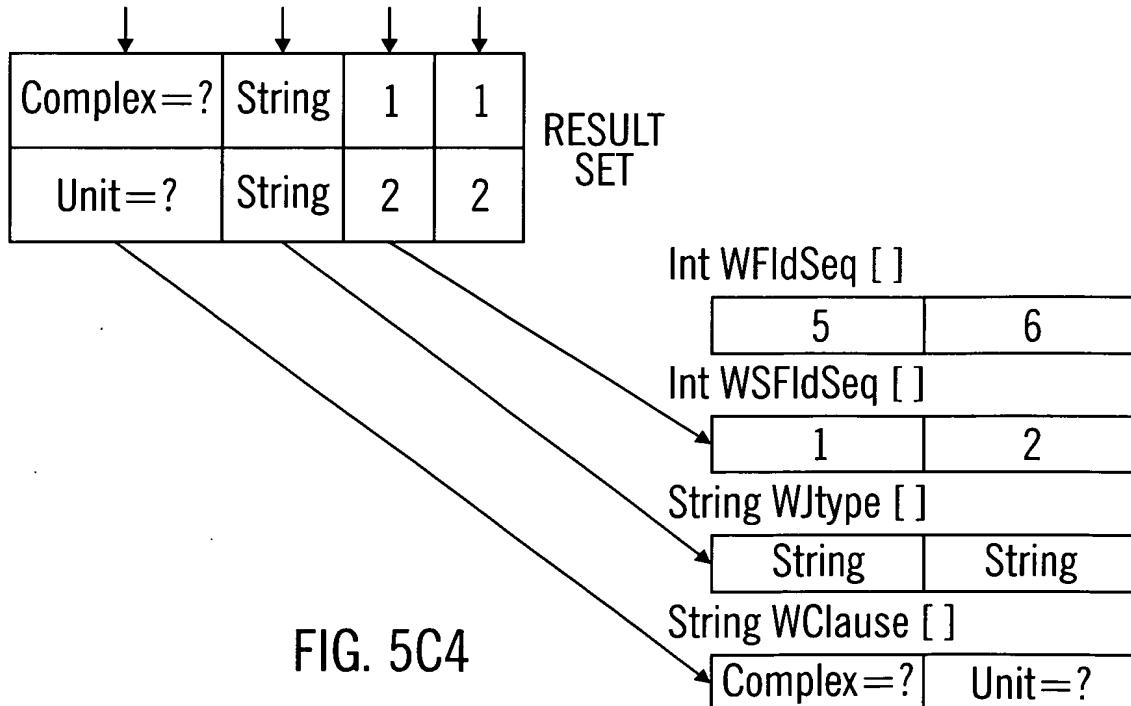
SELECT WCLAUSE, SFLDSEQ, TFLDSEQ FROM UnitStatTab WHERE
WCLAUSE is NOT NULL ORDER BY TFLDSEQ

```
i=1
While not end of resultset
{
// Get values from next row of resultset
WClause[i] = GetString [1]           // get WCLAUSE
WJType[i] = GetString [2]            // get JTYPE
WSFlIdSeq[i] = GetInt [3]           // get SFlIdSeq
WFIdseq[i] = Usize + i             // reset sequence
i++
}
Wsize = i--:
```

575

FIG. 5C3

SELECT WCLAUSE, SFLDSEQ, TFLDSEQ FROM UnitStatTab WHERE WCLAUSE is
NOT NULL ORDER BY TFLDSEQ



12/19

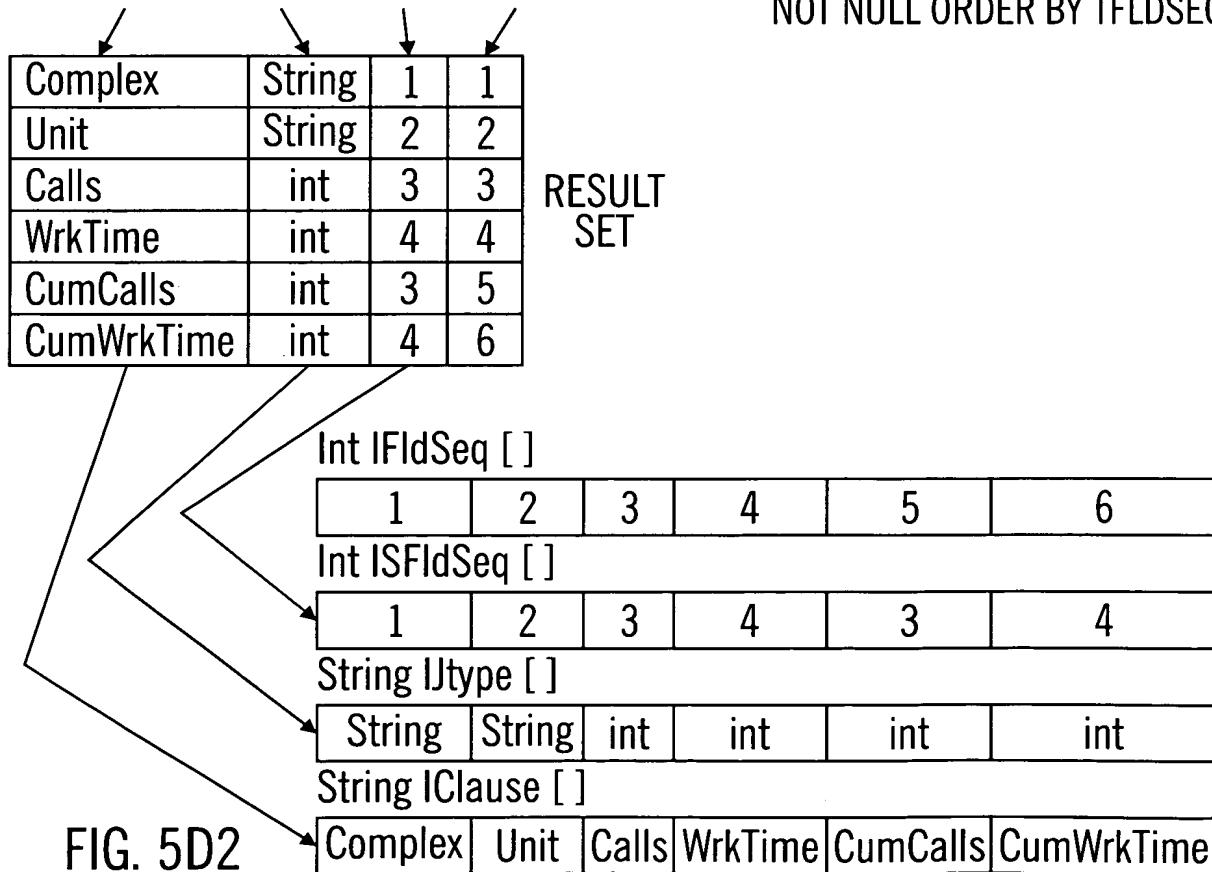
580

SELECT ICLAUSE, JTYPE, SFLDSEQ, TFLDSEQ FROM UnitStatTab WHERE
ICLAUSE is NOT NULL ORDER BY TFLDSEQ

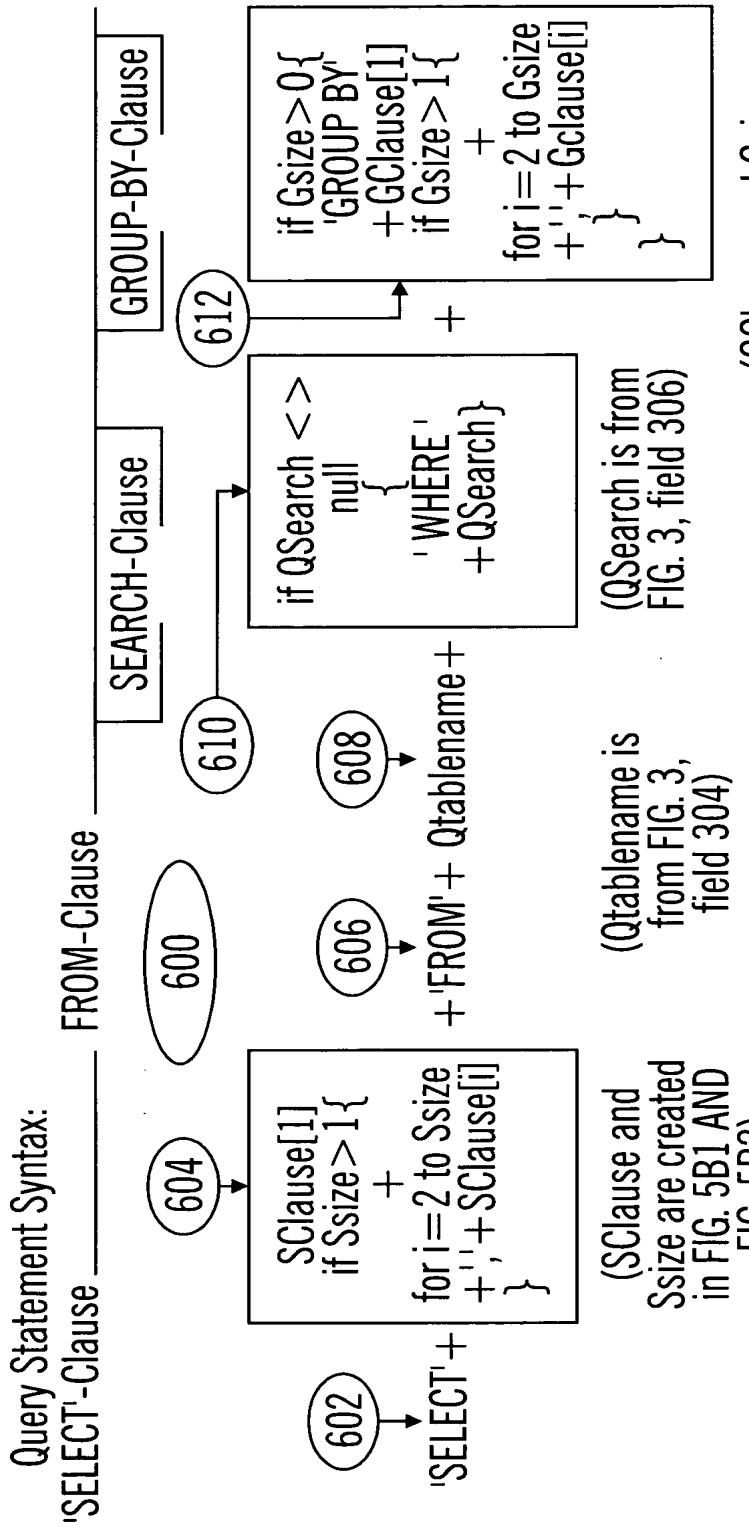
```
i=1
While not end of resultset
{
// Get values from next row of resultset
IClause[i] = GetString [1]           // get ICLAUSE
JType[i] = GetString [2]             // get JTYPE      581
ISFlSeq[i] = GetInt [3]              // get SFlSeq
IFldseq[i] = i                      // reset sequence
i++
}
lsize = i--:
```

FIG. 5D1

SELECT ICLAUSE, JTYPE, SFLDSEQ, TFLDSEQ FROM UnitStatTab WHERE ICLAUSE is
NOT NULL ORDER BY TFLDSEQ



+



(GClause and Gsize are created in FIG. 5B3 and FIG. 5B4)

FIG. 6A1

Select Statement String which was built from 600 above.

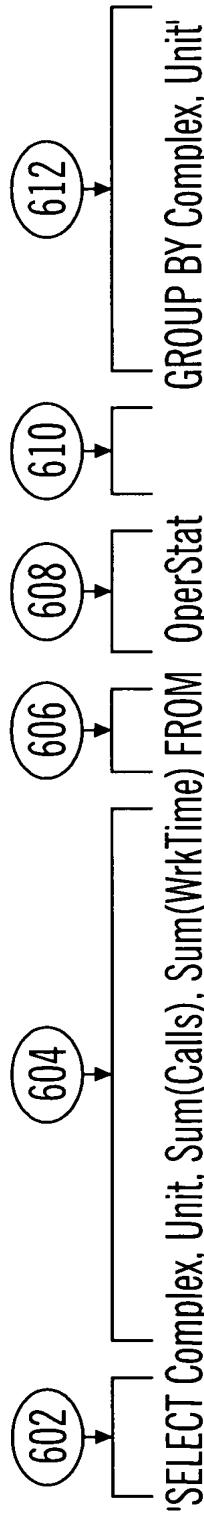


FIG. 6A2

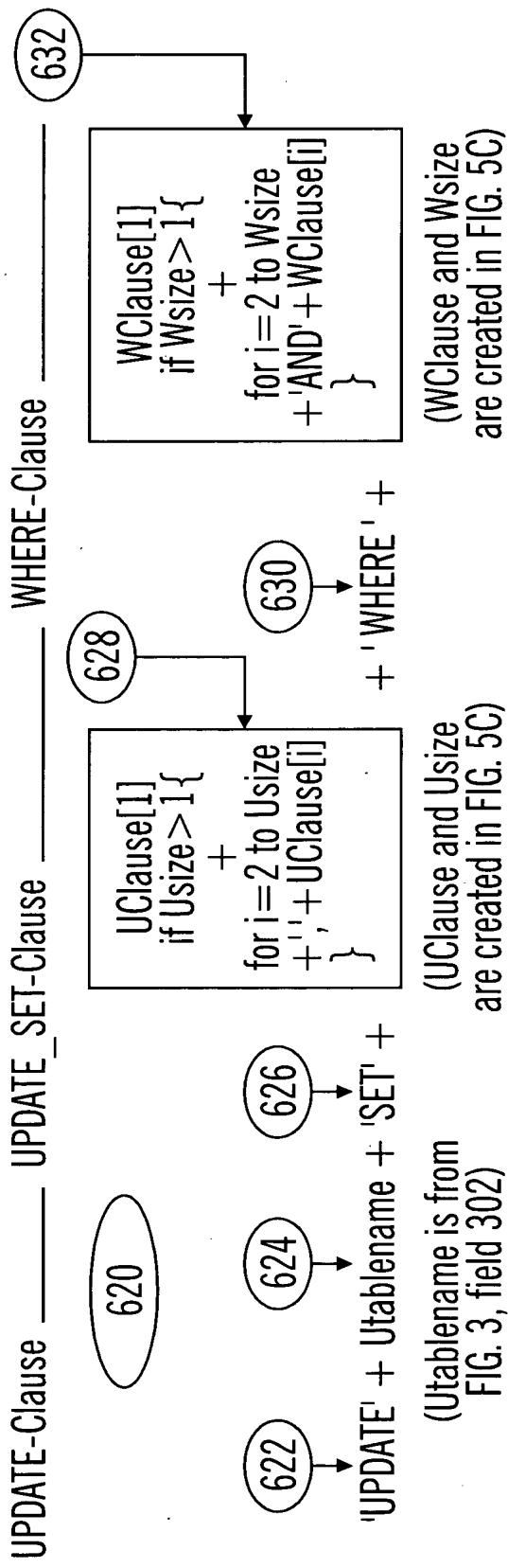


FIG. 6B1

Update Statement String which was built from 620 above.

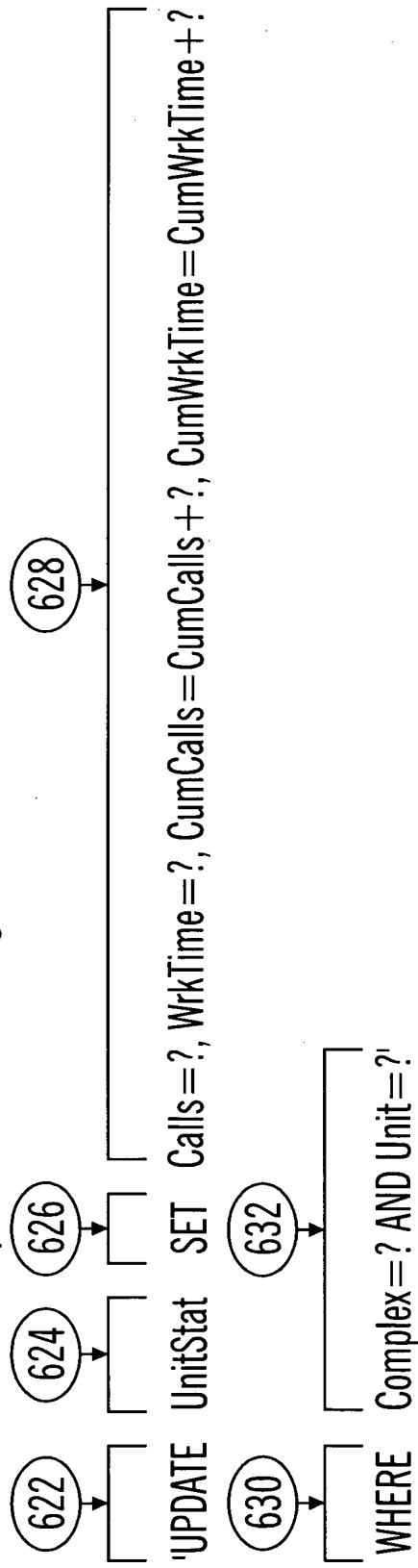


FIG. 6B2

Insert Statement Syntax:
INSERT-Clause _____

- INSERT FIELD-Clause _____ VALUES-Clause _____

```

graph TD
    640((640)) --> 644((644))
    644 --> 642((642))
    642 --> Clause[Clause[1] if lsize>1{  
+ for i=2 to lsize  
+ ',' + [Clause[i]]  
+ }]
    646((646)) --> Clause
    648((648)) --> 652((652))
    652 --> 650((650))

```

The diagram illustrates the control flow of the exploit. The process starts at node 640, which leads to node 644. Node 644 then leads to node 642. Node 642 leads to the code block for the first clause. Following this, node 646 leads to the same clause code block. Next, node 648 leads to node 652. Finally, node 652 leads to node 650.

(IClause and Isize are created in FIG. 5D)

(|size| created in FIG. 5D)

FIG. 6C1

Insert Statement String which was built from 640 above.

```
'INSERT INTO UnitStat (Complex, Unit, Calls, WrkTime, CumCalls, CumWrkTime) VALUES (?,?,?,?,?,?)  
VALUES (642, 644, 646, 648, 650, 652)
```

FIG. 6C2

16/19

550

'SELECT Complex, Unit, Sum(Calls), Sum(WrkTime) FROM OperStat
GROUP BY Complex, Unit'

```
For i=1 to Ssize
{
    j=SFlSeq[i]
    if SJType[i]='String'
        StringRS[j]=GetString[i]
    else
        IntRS[j]=GetInt[i]
}
```

FIG. 7A

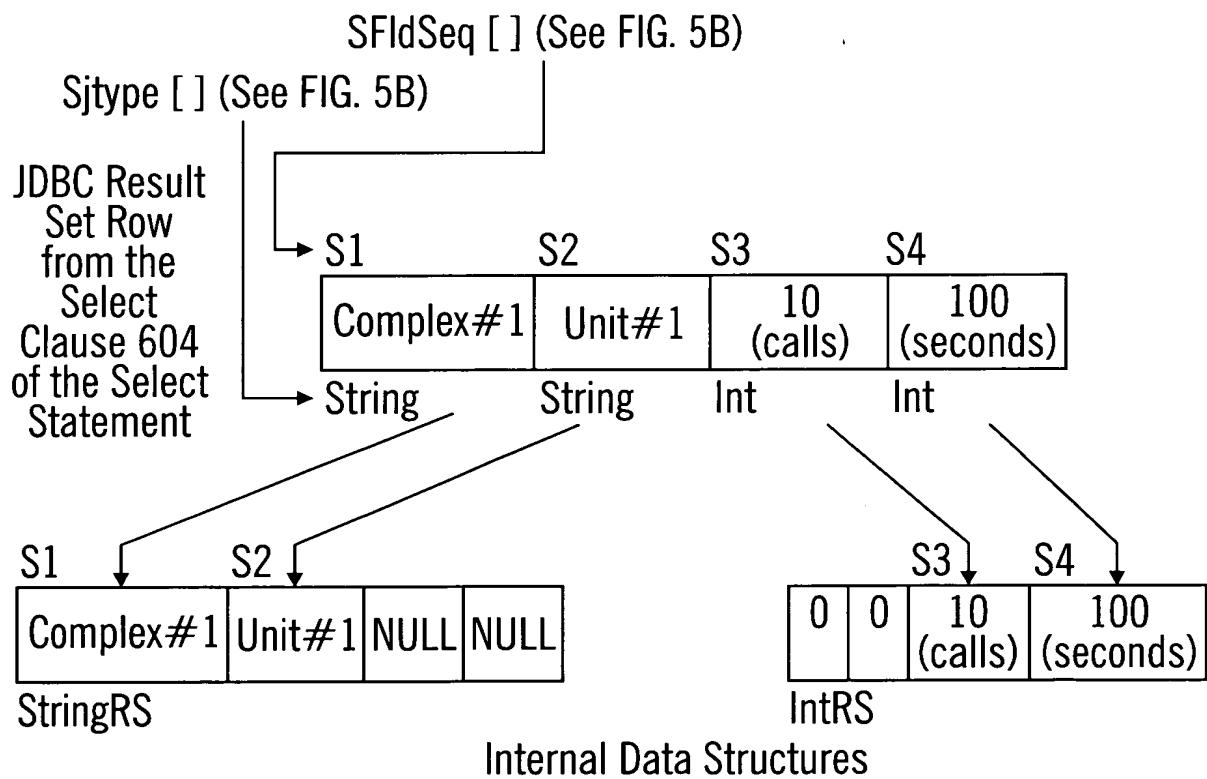


FIG. 7B

17/19

'UPDATE UnitStat SET Calls=? , WrkTime=? , CumCalls=CumCalls + ?
U1 U2 U3
CumWrkTime=CumWrkTime + ?
U4
WHERE Complex=? AND Unit=?
U5 U6

```
For i=1 to Usize
{
  j=UFlIdSeq[i]
  k=USFlIdSeq[i]
  if UJType[i]='String'
    setString[j]=StringRS[k]
  else
    setint[j]=IntRS[k]
}
```

FIG. 8A1

```
For i=1 to Wsize
{
  j=WFlIdSeq[i]
  k=WSFlIdSeq[i]
  if WJType[i]='String'
    setString[j]=StringRS[k]
  else
    setint[j]=IntRS[k]
}
```

FIG. 8A2

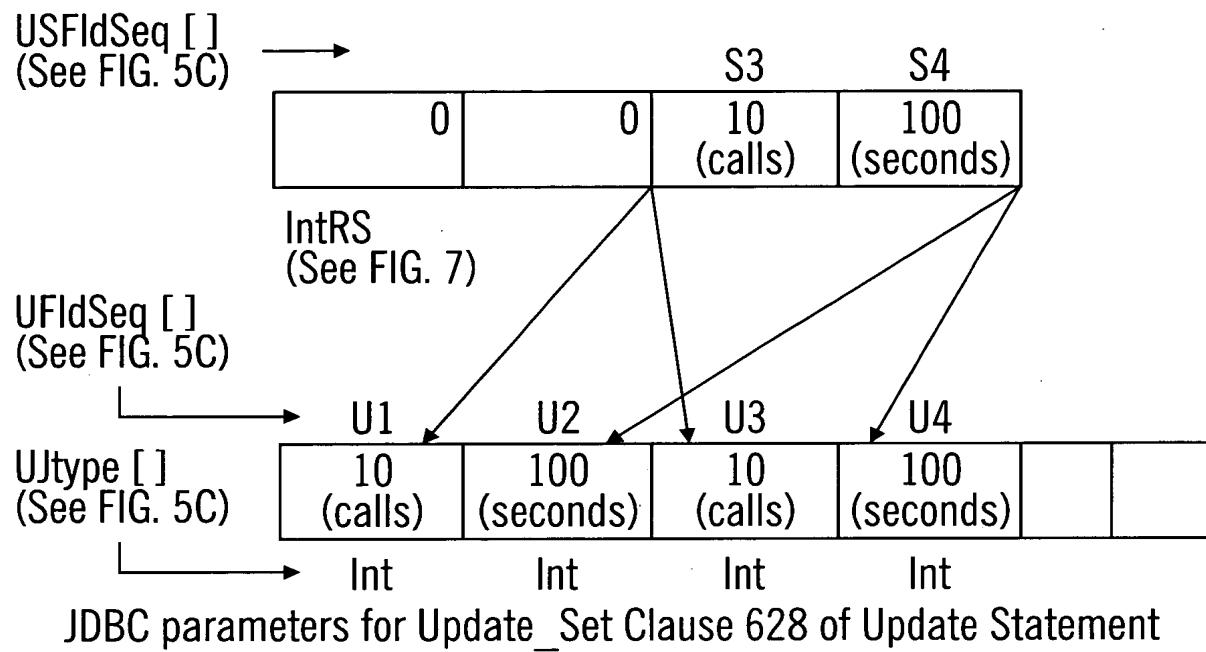


FIG. 8A3

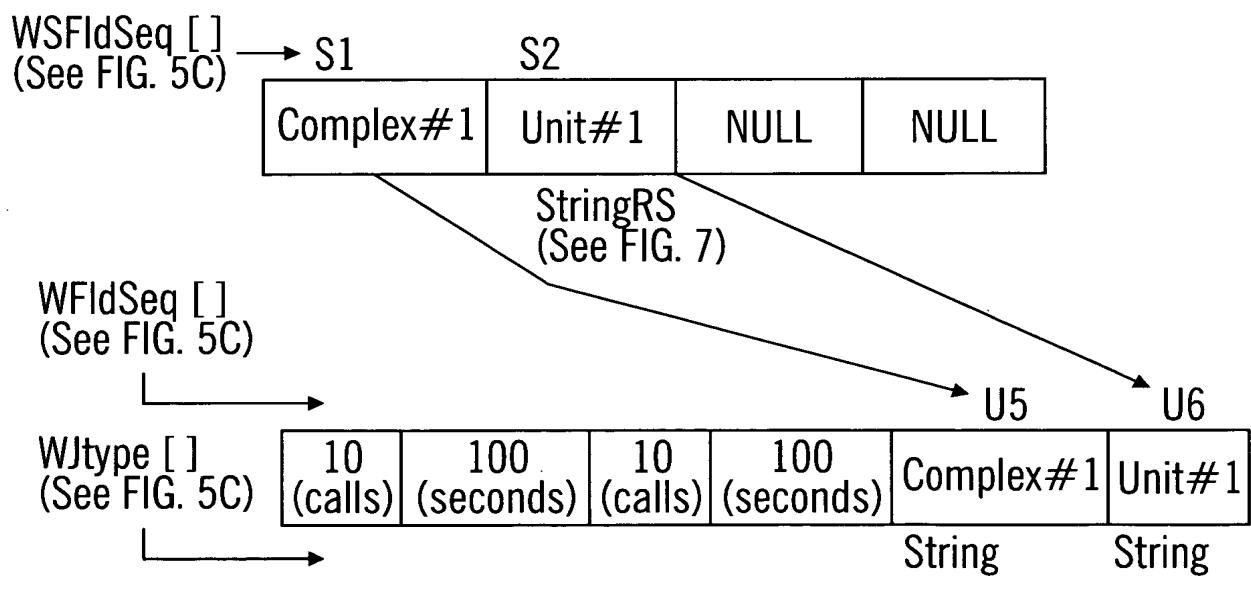


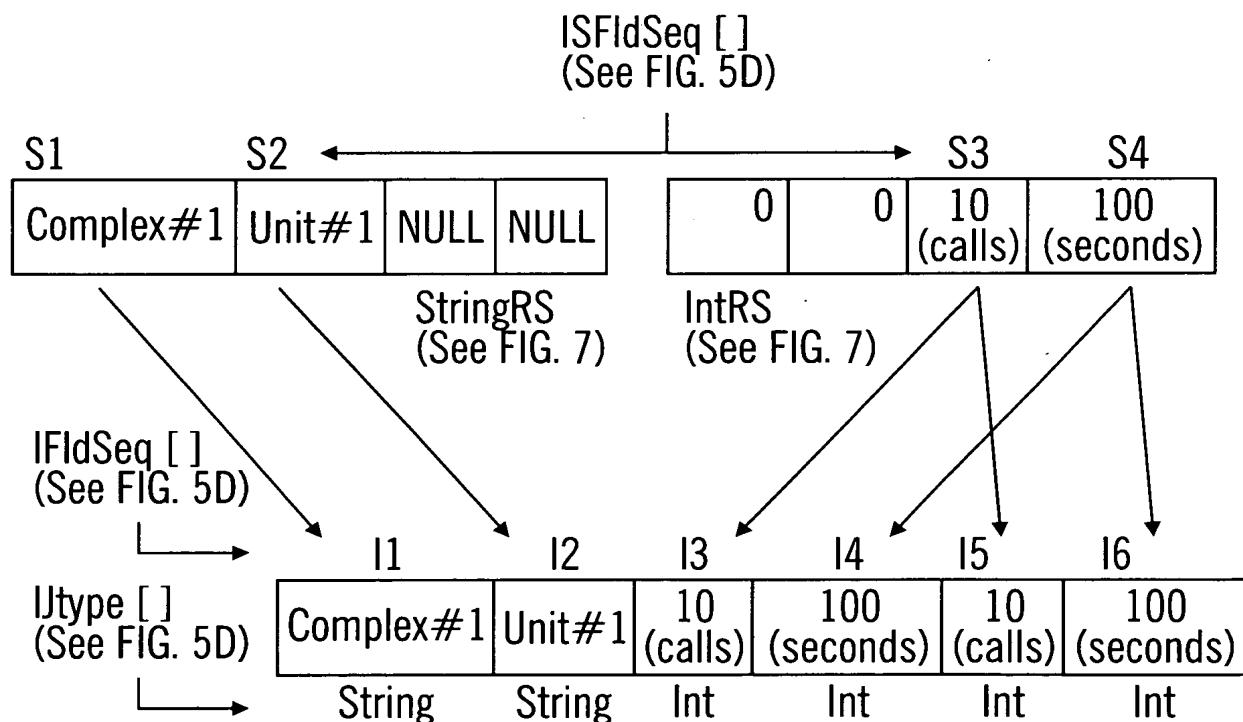
FIG. 8A4

19/19

'INSERT INTO UnitStat(Complex, Unit, Calls, WrkTime, CumCalls, CumWrkTime) VALUES (?, ?, ?, ?, ?, ?)'
 I1,I2,I3,I4,I5,I6

```
For i=1 to lsize
{
    j=IFldSeq[i]
    k=ISFldSeq[i]
    if IJType[i]='String'
        setString[j]=StringRS[k]
    else
        setint[j]=IntRS[k]
}
```

FIG. 9A



JDBC parameters for Values Clause 650 of Insert Statement

FIG. 9B